

Social Media and the New Information Battlefield

Author: Reza Khan

Date: 27 August 2026

Theme: Strategic Communications | Information Security

Pakistan's information environment is undergoing a structural change: social media is no longer merely a distribution channel for news but a contested space in which political actors, state institutions, journalists, activists, anonymous networks and increasingly sophisticated AI tools compete to shape public understanding. The central strategic problem is therefore not simply the existence of false information. It is the widening gap between the speed at which a narrative can be created and amplified and the time required to verify whether it is true. As that gap grows, public trust itself becomes a strategic asset and a potential target.

1. Context

Pakistan's digital public sphere has expanded rapidly. According to DataReportal's Digital 2026: Pakistan report, there were 117 million internet users in Pakistan in October 2025, while the country had 79.9 million social media user identities, equivalent to 31.2 percent of the population. DataReportal also records a 25 percent year on year increase in social media user identities. These figures should not be treated as a count of unique individuals, because platform data and advertising audiences have methodological limitations, but they demonstrate the scale of the environment in which political and social narratives now circulate. [\[DataReportal\]](#)

The significance of this expansion is not simply that more Pakistanis can publish or consume information. The architecture of social media has changed the sequence through which information becomes accepted as knowledge. A photograph, short video, voice recording or screenshot can be circulated before its source is known; television channels and online news outlets may then respond to the viral material; and the original claim can become the reference point against which subsequent corrections are judged. Verification has increasingly become a second stage activity, while narrative formation is immediate.

The problem has become more difficult with the arrival of generative artificial intelligence. The January 2026 iVerify Pakistan report, launched by the Centre for Excellence in Journalism at IBA Karachi, examined 1,026 potentially false or misleading claims from December 2023 through November 2025, with 513 claims subjected to detailed verification. The report identified deep fakes, doctored content, distorted context, mistranslation, impersonation and AI-generated material among the techniques being used to mislead audiences. It also identified social platforms, particularly X.com, as important amplifiers, while encrypted messaging platforms such as WhatsApp remain difficult to observe despite their influence on public opinion. [\[iVerify Pakistan\]](#)

2. Analysis

The first strategic shift is from an information environment organised around scarcity to one organised around abundance and speed. In the traditional media model, editorial institutions performed a filtering function before information reached a mass audience. Social media has redistributed that filtering function to algorithms, networks of users and individual accounts. The result is not the disappearance of gatekeepers but the creation of different gatekeepers; ones whose incentives are often based on engagement, novelty, outrage and repetition rather than accuracy.

This is why the phrase 'information battlefield' is more useful than simply 'misinformation problem'. Competing actors do not merely attempt to persuade audiences; they seek to establish the frame through which subsequent facts will be interpreted. During a political dispute, the first widely circulated video may determine whether an event is understood as a protest, a crackdown, an act of violence or an isolated incident. During a security crisis, an old photograph presented as current can generate panic or false confidence before authorities have time to establish what happened. During an international crisis, fabricated maps, satellite images or AI-generated footage can create the appearance of evidence where none exists.

The technological problem is therefore only half the problem. The other half is institutional credibility. Pakistan's Ministry of Information and Broadcasting explicitly assigns its Digital Communication Department responsibility for monitoring online media, identifying unverified or baseless claims, and countering propaganda and fake news. The

government has also continued to develop institutional capacity around information integrity. In January 2026, the National CERT brought officials from 20 federal ministries and attached departments together for training on information integrity, hostile information threats, disinformation and narrative manipulation. [\[MoIB\]](#) [\[National CERT\]](#)

These developments are important, but a purely reactive model has inherent limits. An institution that responds only after a false claim has gone viral is operating at a structural disadvantage. It is also not enough to issue a denial. A credible response has to answer the claim, provide evidence, identify what is known and unknown, and reach the same audiences through channels capable of competing with the original narrative. The objective should be to reduce the information advantage enjoyed by whoever publishes first.

There is also a danger in treating information integrity as synonymous with control of information. Removing content, restricting platforms or relying exclusively on official sources may sometimes address an immediate security concern, but they do not automatically create public trust. Where citizens already distrust institutions, a heavy handed response can reinforce the belief that authorities are attempting to suppress information rather than establish facts. The stronger long term approach is a credible verification ecosystem involving government, independent journalism, academia, technology platforms and civil society.

The changing nature of synthetic media makes this particularly urgent. Reuters reported in April 2026 on a convincing deep fake involving journalist Yalda Hakim and a fabricated interview concerning Pakistan. The incident demonstrated a new dimension of the problem: a false video can borrow the credibility of a trusted journalist or institution, making the deception more persuasive than an obviously fabricated anonymous post. As AI-generated media becomes cheaper and more realistic, the old assumption, 'seeing is believing' becomes increasingly unreliable. [\[Reuters\]](#)

The strategic consequence is a shift from a battle over individual facts to a battle over the credibility of the entire information system. If citizens become convinced that every video can be fake, every official statement can be propaganda and every journalist can be manipulated, then misinformation does not have to establish a particular falsehood. It can simply create enough uncertainty to make people disengage from reliable information. This is arguably the more serious threat because institutional trust is much harder to rebuild than a single false claim is to correct.

3. Implications

The implications extend across government, security, business and society. Government institutions face a shorter response window during crises: delays that might once have been measured in hours can now be consequential within minutes. Security agencies must account for the possibility that operational events will be accompanied by manipulated footage, false claims and deliberate attempts to expose or distort sensitive information. Businesses face reputational and financial risks when false claims about products, companies or executives spread faster than corporate communications teams can respond. Journalists face an increasingly difficult verification burden because publishing quickly can create pressure to repeat material that has not been authenticated, while publishing cautiously can mean losing the attention cycle. Citizens face the greatest cumulative risk: information overload can encourage people to rely on identity, emotion and group loyalty as shortcuts for deciding what to believe.

4. The Way Forward

Pakistan should build information integrity as a permanent institutional capability rather than treating each misinformation episode as an isolated communications crisis. Government departments should maintain rapid verification cells that can distinguish verified facts, credible but incomplete information and demonstrably false claims, and should publish evidence alongside corrections wherever possible. Official digital content should increasingly use provenance measures, metadata and verifiable source documentation so that authentic material is easier to distinguish from manipulated material. National CERT has already recommended measures including digital watermarks, metadata validation, cooperation with platforms and public digital literacy initiatives; these should be developed into routine institutional practice. [\[National CERT advisory\]](#)

At the same time, the response cannot rest with government. Independent fact checkers, universities, journalists and civil society organisations should develop shared verification protocols and public education programmes that

teach citizens how to assess sources, dates, locations, original uploads and manipulated media. The iVerify model is valuable precisely because it combines verification with institutional and media partnerships. The long term objective should not be to create a public that believes official information automatically. It should be to create a public that is capable of distinguishing evidence from assertion, regardless of who is making the assertion. [\[iVerify\]](#)

Sources

- DataReportal — Digital 2026: Pakistan — <https://datareportal.com/reports/digital-2026-pakistan>
- Centre for Excellence in Journalism, IBA Karachi — iVerify Pakistan report launch, January 2026 — <https://cej.iba.edu.pk/iverify-report-launch-jan-26.php>
- Ministry of Information and Broadcasting, Government of Pakistan — Digital Communication Department — <https://www.moib.gov.pk/Pages/163/CW>
- National CERT Pakistan — Information Integrity and Countering Hostile Information Threats — <https://pkcert.gov.pk/images-gallery/ncert-conducts-comprehensive-training-information-integrity-01-2026.asp>
- National CERT Pakistan — Advisory on synthetic media and information integrity — <https://pkcert.gov.pk/advisory/25/24.pdf>
- Reuters — Yalda Hakim on the collapse of 'seeing is believing', April 2026 — <https://www.reuters.com/lifestyle/culture-current/yalda-hakim-collapse-seeing-is-believing-2026-04-25/>
- Haroon et al. — Investigating Misinformation Dissemination on Social Media in Pakistan — <https://arxiv.org/abs/2106.09338>
- Ali & Qazi — Countering Misinformation on Social Media Through Educational Interventions: Evidence from Pakistan — <https://arxiv.org/abs/2107.02775>

About the Author

Reza Khan is a researcher with an M.Phil. in Government and Public Policy from the National Defence University, Islamabad, and an MBA in Finance. His professional experience spans business strategy, international trade, economics and organizational leadership, and he has taught Development Economics, Microeconomics and Supply Chain Management at the University of London Global MBA programme. His analytical interests include public policy, governance, strategic communication and the interaction between technology, institutions and society.